UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/997,045	11/28/2001	Khoi Hoang	60595-301301	3497

7590 10/06/2004

Brian R. Coleman
Patent Attorney
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 95026-2168

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/997,045	HOANG, KHOI
	Examiner	Art Unit
	Justin T. Darrow	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-40 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-40 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 November 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-40 have been examined.

Information Disclosure Statement

2. The information disclosure statements (IDS) filed on 03/21/2003 and 08/14/2003 are in compliance with the provisions of 37 CFR 1.97. Accordingly, these information disclosure statements have been considered by the examiner and an initialed copy of each one has been attached to this Office action.

Claim Objections

3. Claim 8 is objected to because of the following informality: after "parameter:" in page 12, lines 30, insert --and--. Appropriate correction is required.

4. Claim 9 is objected to because of the following informality: after "parameter:" in page 13, lines 33, insert --and--. Appropriate correction is required.

5. Claim 24 is objected to because of the following informality: after "parameter:" in page 14, lines 31, insert --and--. Appropriate correction is required.

6. Claim 32 is objected to because of the following informality: after "parameter:" in page 15, lines 34, insert --and--. Appropriate correction is required.

7. Claim 40 is objected to because of the following informality: after "parameter:" in page 16, lines 32, insert --and--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 33-40 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for generating a second array of decrypting keys as a function of a first array of decrypting keys (see specification, page 9, lines 24-27; figure 8, step 12), does not reasonably provide enablement for generating a second array of decrypting keys as a function of the first decrypting key. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims. The specification does not satisfy the enablement requirement necessitating undue experimentation because the nature of the invention. See MPEP § 2164.01(a) and In re Wands, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988). This rejection can be overcome by deleting "encrypting key" in page 16, line 6 and replacing with -- array of encrypting keys --.

10. Claim 40 is rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for generating a second array of decrypting keys as a function of a first array of decrypting keys (see specification, page 9, lines 24-27; figure 8, step 12), does not reasonably provide enablement for generating a second array of decrypting keys as a function of the first decrypting key. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention

commensurate in scope with these claims. The specification does not satisfy the enablement requirement necessitating undue experimentation because the nature of the invention. See MPEP § 2164.01(a) and In re Wands, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988). This rejection can be overcome by deleting "decrypting key" in page 16, line 31 and replacing with -- array of decrypting keys --.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "the first decrypting key" in page 12, lines 29. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "decryption" in page 12, line 28 and replacing with --decrypting--.

13. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 recites the limitation "the encryption scheme" in page 13, line 10. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encryption scheme is" in page 13, line 10 and replacing with --decrypting step corresponds to--.

14. Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 13 recites the limitation "the encryption scheme" in page 13, line 15. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encryption scheme is" in page 13, line 15 and replacing with --decrypting step corresponds to--.

15. Claim 16 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 16 recites the limitation "the encrypted data message" in page 13, lines 23. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encrypted" in page 13, line 23.

16. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 24 recites the limitation "the first decrypting key" in page 14, lines 30. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "decryption" in page 14, line 29 and replacing with --decrypting--.

17. Claim 27 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 27 recites the limitation "the encryption scheme" in page 15, line 14. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encryption scheme is" in page 15, line 14 and replacing with --decrypting step corresponds to--.

18. Claim 29 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 29 recites the limitation "the encryption scheme" in page 15, line 20. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encryption scheme is" in page 15, line 20 and replacing with --decrypting step corresponds to--.

19. Claim 32 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 32 recites the limitation "the encrypted data message" in page 15, lines 30. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "encrypted" in page 15, line 30.

20. Claims 33-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 33 recites the limitation "the first encrypting key" in page 16, lines 6. There is insufficient antecedent basis for this limitation in the claim.

21. Claim 40 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 40 recites the limitation "the first decrypting key" in page 14, lines 30. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by deleting "decryption" in page 16, line 30 and replacing with --decrypting--.

Claim Rejections - 35 USC § 102

22. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

23. Claims 1, 4, 5, 7-9, 12, 13, 15-17, 20, 21, 23-25, 28, 29, 31-33, 36, 37, 39, and 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski et al., U.S. Patent No. 5,341,425 A.

As per claim 1, Wasilewski et al. depict a method for securely transmitting a data message, comprising:

obtaining a first encrypting key (see column 4, lines 67-8; column 5, line 1; figure 2, items 40, 22, 24, and 28; providing a system key as a first encrypting key that is common to each transmission site);

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 5, lines 24-28; figure 2, items 40, 42, 44, 48, 50, and 52; means for convolving the system key, as the first encrypting key, and the broadcast key unique to that site, as an identified parameter, to generate a unique data encryption key as a second encrypting key);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 6, lines 1-4; figure 2, items 32, 34, 38, 52, and 54; encrypting a data set as a message with the unique data encryption key as a second encrypting key); and

transmitting the encrypted data message (see column 6, lines 17-22; figure 2, items 54, 56, 58; coupling the output of the encryptor as an encrypted data message for transmission).

As per claim 4, Wasilewski et al. further point out:

that the encrypting step corresponds to a private key encryption scheme (see column 6, lines 8-18; figure 2, items 52 and 54; the encryptor may be a stream cipher or a block cipher using the unique data encryption key as a private encryption key).

As per claim 5, Wasilewski et al. also specify:

that the encryption scheme is a DES scheme (see column 6, lines 11-16; figure 2, item 54; the encryptor may implement the Digital Encryption Standard (DES) algorithm).

As per claim 7, Wasilewski et al. then discuss:

that the identified parameter is a randomly generated number (see column 12, lines 46-47; figure 5, items 142, 144, 148, 150, and 154; a pseudorandom bit generator producing a pseudorandom value to generate a key).

As per claim 8, Wasilewski et al. next elaborate:

receiving the encrypted data message (see column 6, lines 48-50; figure 2, item 30; the encrypted data sets as encrypted data messages are transmitted to a reception site);

obtaining a first decrypting key (see column 7, lines 24-25; figure 2, item 40; retrieving the system key as a first decryption key);

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 40-44; figure 2, items 42, 44, 48, 40, 72, and 74; convolving the retrieved system key as the first decrypting key, and the retrieved broadcast key, as the identified parameter, to reproduce the unique encryption key employed at the selected transmission site, as the second decrypting key);

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 59-63; figure 2, items 74, 64, and 62; decrypting the encrypted data set with the reproduced encryption key).

As per claim 9, Wasilewski et al. illustrate a method for securely receiving a data message, comprising:

obtaining a first decrypting key (see column 7, lines 24-25; figure 2, item 40; retrieving the system key as a first decryption key);

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 40-44; figure 2, items 42, 44, 48, 40, 72, and 74; convolving the retrieved system key as the first decrypting key, and the retrieved broadcast key, as the identified parameter, to reproduce the unique encryption key employed at the selected transmission site, as the second decrypting key); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 59-63; figure 2, items 74, 64, and 62; decrypting the encrypted data set with the reproduced encryption key).

As per claim 12, Wasilewski et al. further point out:

that the decrypting step corresponds to a private key encryption scheme (see column 6, lines 8-18; figure 2, items 52 and 54; the encryptor may be a stream cipher or a block cipher using the unique data encryption key as a private encryption key).

As per claim 13, Wasilewski et al. also specify:

that the decrypting step corresponds to a DES scheme (see column 6, lines 11-16; figure 2, item 54; the encryptor may implement the Digital Encryption Standard (DES) algorithm).

As per claim 15, Wasilewski et al. then discuss:

that the identified parameter is a randomly generated number (see column 12, lines 46-47; figure 5, items 142, 144, 148, 150, and 154; a pseudorandom bit generator producing a pseudorandom value to generate a key).

As per claim 16, Wasilewski et al. then depict

that the data message is generated by a method, comprising:

obtaining a first encrypting key (see column 4, lines 67-8; column 5, line 1; figure 2, items 40, 22, 24, and 28; providing a system key as a first encrypting key that is common to each transmission site);

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 5, lines 24-28; figure 2, items 40, 42, 44, 48, 50, and 52; means for convolving the system key, as the first encrypting key, and the broadcast key unique to that site, as an identified parameter, to generate a unique data encryption key as a second encrypting key);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 6, lines 1-4; figure 2, items 32, 34, 38, 52, and 54; encrypting a data set as a message with the unique data encryption key as a second encrypting key); and

transmitting the encrypted data message (see column 6, lines 17-22; figure 2, items 54, 56, 58; coupling the output of the encryptor as an encrypted data message for transmission).

As per claim 17, Wasilewski et al. depict a communication system for securely transmitting a data message, comprising:

a memory (see column 5, lines 1-17; figure 2, items 40, 42, 44, and 48; system key and broadcast keys stored in the transmission site in a memory);

a processor configured to execute the steps (see column 5, lines 63-68; column 6, lines 1-4; figure 2, items 50 and 54; a convolving means in combination with an encryptor) comprising:

obtaining a first encrypting key (see column 4, lines 67-8; column 5, line 1; figure 2, items 40, 22, 24, and 28; providing a system key as a first encrypting key that is common to each transmission site);

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 5, lines 24-28; figure 2, items 40, 42, 44, 48, 50, and 52; means for convolving the system key, as the first encrypting key, and the broadcast key unique to that site, as an identified parameter, to generate a unique data encryption key as a second encrypting key);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 6, lines 1-4; figure 2, items 32, 34, 38, 52, and 54; encrypting a data set as a message with the unique data encryption key as a second encrypting key); and

a transmitter (see column 17-22; figure 2, item 56; a combiner/transmitter) for transmitting the encrypted data message (see column 6, lines 17-22; figure 2, items 54, 56, 58; coupling the output of the encryptor as an encrypted data message for transmission).

As per claim 20, Wasilewski et al. further point out:

that the encrypting step corresponds to a private key encryption scheme (see column 6, lines 8-18; figure 2, items 52 and 54; the encryptor may be a stream cipher or a block cipher using the unique data encryption key as a private encryption key).

As per claim 21, Wasilewski et al. also specify:

that the encryption scheme is a DES scheme (see column 6, lines 11-16; figure 2, item 54; the encryptor may implement the Digital Encryption Standard (DES) algorithm).

As per claim 23, Wasilewski et al. then discuss:

that the identified parameter is a randomly generated number (see column 12, lines 46-47; figure 5, items 142, 144, 148, 150, and 154; a pseudorandom bit generator producing a pseudorandom value to generate a key).

As per claim 24, Wasilewski et al. next elaborate:

receiving the encrypted data message (see column 6, lines 48-50; figure 2, item 30; the encrypted data sets as encrypted data messages are transmitted to a reception site);

obtaining a first decrypting key (see column 7, lines 24-25; figure 2, item 40; retrieving the system key as a first decryption key);

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 40-44; figure 2, items 42, 44, 48, 40, 72, and 74; convolving the retrieved system key as the first decrypting key, and the retrieved broadcast key, as the identified parameter, to reproduce the unique encryption key employed at the selected transmission site, as the second decrypting key);

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 59-63; figure 2, items 74, 64, and 62; decrypting the encrypted data set with the reproduced encryption key).

As per claim 25, Wasilewski et al. illustrate a communication system for securely receiving a data message, comprising:

a memory (see column 6, lines 50-54; figure 2, item 60; a memory for storing the system key and broadcast keys);

a receiver configured to receive an encrypted data message (see column 7, lines 4-8; figure 2, item 62; a receiver for receiving the encrypted sets of data); and

a processor configured to execute the steps (see column 7, lines 40-63; figure 2, items 72 and 64; a convolver means in combination with a decryptor) comprising:

obtaining a first decrypting key (see column 7, lines 24-25; figure 2, item 40; retrieving the system key as a first decryption key);

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 40-44; figure 2, items 42, 44, 48, 40, 72, and 74; convolving the retrieved system key as the first decrypting key, and the retrieved broadcast key, as the identified parameter, to reproduce the unique encryption key employed at the selected transmission site, as the second decrypting key); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 59-63; figure 2, items 74, 64, and 62; decrypting the encrypted data set with the reproduced encryption key).

As per claim 28, Wasilewski et al. further point out:

that the decrypting step corresponds to a private key encryption scheme (see column 6, lines 8-18; figure 2, items 52 and 54; the encryptor may be a stream cipher or a block cipher using the unique data encryption key as a private encryption key).

As per claim 29, Wasilewski et al. also specify:

that the decrypting step corresponds to a DES scheme (see column 6, lines 11-16; figure 2, item 54; the encryptor may implement the Digital Encryption Standard (DES) algorithm).

As per claim 31, Wasilewski et al. then discuss:

that the identified parameter is a randomly generated number (see column 12, lines 46-47; figure 5, items 142, 144, 148, 150, and 154; a pseudorandom bit generator producing a pseudorandom value to generate a key).

As per claim 32, Wasilewski et al. then depict

a transmitter (see column 17-22; figure 2, item 56; a combiner/transmitter) configured to transmit the encrypted data message (see column 6, lines 17-22; figure 2, items 54, 56, 58; coupling the output of the encryptor as an encrypted data message for transmission);

a second processor configured to execute the steps (see column 5, lines 63-68; column 6, lines 1-4; figure 2, items 50 and 54; a convolving means in combination with an encryptor) comprising:

obtaining a first encrypting key (see column 4, lines 67-8; column 5, line 1; figure 2, items 40, 22, 24, and 28; providing a system key as a first encrypting key that is common to each transmission site);

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 5, lines 24-28; figure 2, items 40, 42, 44, 48, 50, and 52; means for convolving the system key, as the first encrypting key, and the broadcast key unique to that site, as an identified parameter, to generate a unique data encryption key as a second encrypting key); and

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 6, lines 1-4; figure 2, items 32, 34, 38, 52, and 54; encrypting a data set as a message with the unique data encryption key as a second encrypting key).

As per claim 33, Wasilewski et al. show a method for securely transmitting a data message, comprising:

obtaining a first array of encrypting keys (see column 12, lines 3-7; figure 5, items 142, 144, 148; providing broadcast keys in an array; see column 11, lines 62-65; figure 5, items 132, 134, and 138; where a respective broadcast key is unique to a data set);

generating a second array of encrypting keys as a function of the first array of encrypting keys and as a function of an identified parameter (see column 12, lines 30-37; figure 5, items 140, 142, 144, 148, and 150; generating a unique data encryption key array by convolving the array of broadcast keys with the system key);

encrypting the data message using the second array of encrypting keys to generate an encrypted data message (see column 12, lines 35-37; figure 5, items 152, 154, 132, 134, and 138; encrypting the data with each unique data encryption key from the array); and

transmitting the encrypted data message (see column 12, lines 54-58; figure 5, item 156; combining the encrypted data sets into an encrypted message and transmitting it to a reception site).

As per claim 36, Wasilewski et al. further point out:

that the encrypting step corresponds to a private key encryption scheme (see column 6, lines 8-18; figure 2, items 52 and 54; the encryptor may be a stream cipher or a block cipher using the unique data encryption key as a private encryption key).

As per claim 37, Wasilewski et al. also specify:

that the encryption scheme is a DES scheme (see column 12, lines 49-52; figure 5, item 154; the encryptor may implement the Digital Encryption Standard (DES) algorithm).

As per claim 39, Wasilewski et al. then discuss:

that the identified parameter is a randomly generated number (see column 12, lines 46-47; figure 5, items 142, 144, 148, 150, and 154; a pseudorandom bit generator producing a pseudorandom value to generate a key).

As per claim 40, Wasilewski et al. further point out:

receiving the encrypted data message (see column 12, lines 54-58; figure 5, item 156; figure 1, item 30; transmitting the combined encrypted data sets to a reception site);

obtaining a first array of decrypting keys (see column 7, lines 24-28; figure 2, items 42, 44, and 48; retrieving broadcast keys corresponding to each encrypted data set);

generating a second array of decrypting keys as a function of the first array of decrypting keys and as a function of the identification parameter (see column 7, lines 40-44; figure 2, items 42, 44, 48, 70, 72, and 74; convolving the array of broadcast keys with the system key to reproduce the encryption key); and

decrypting the encrypted data message using the second array of decrypting keys to recover the data message (see column 13, lines 3-11; decrypting the encrypted combined data sets as an encrypted message; column 7, lines 59-63; figure 2, item 64; decrypting the received encrypted data set).

24. Claims 1-3, 8-11, 16-19, 24-27, and 32 are rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan et al., U.S. Patent No. 5,588,061 A.

As per claim 1, Ganesan et al. depict a method for securely transmitting a data message, comprising:

obtaining a first encrypting key (see column 7, lines 5-9; figure 2, step 200; generating a private exponent key d_{ij});

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the

private key so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 7, lines 36-38; singing a message m using di to form the signature $s_i = m^{di} \bmod N_i$); and

transmitting the encrypted data message (see column 7, lines 39-40; figure 2, step 212; transmitting the signed message s_i).

As per claims 2 and 3, Ganesan et al. further show:

that the encryption step corresponds to an RSA public key encryption scheme (see column 7, lines 35-39; figure 2, step 210; signing the message with a private RSA key).

As per claim 8, Ganesan et al. next elaborate:

receiving the encrypted data message (see column 7, lines 39-40; figure 2, step 212; sending the signed message s_i to a server);

obtaining a first decrypting key (see column 7, lines 5-9; figure 2, step 200; generating the public and private exponent key d_{ij});

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key to obtain d_j so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 40-47; figure 2, steps 214 and 216; performing signature verification including jointly signing the signed message $s_{ij} = s_i^{dji} \bmod N_i$ with dj and completing the verification by decrypting s_{ij} to verify that $s_{ij}^{eij} \bmod N = m^{didjeij} \bmod N_{ij} = m$).

As per claim 9, Ganesan et al. describe a method for securely receiving a data message, comprising:

obtaining a first decrypting key (see column 7, lines 5-9; figure 2, step 200; generating the public and private exponent key d_{ij});

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key to obtain d_j so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 40-47; figure 2, steps 214 and 216; performing signature verification including jointly signing the signed message $s_{ij} = s_i^{dji} \bmod N_i$ with dj and completing the verification by decrypting s_{ij} to verify that $s_{ij}^{eij} \bmod N = m^{didjeij} \bmod N_{ij} = m$).

As per claims 10 and 11, Ganesan et al. further explain:

that the decrypting step corresponds to an RSA public key scheme (see column 7, lines 35-39; figure 2, step 210; signing the message with a private RSA key).

As per claim 16, Ganesan et al. additionally elaborate:

that the encrypted data message is generated by a method comprising:

obtaining a first encrypting key (see column 7, lines 5-9; figure 2, step 200; generating a private exponent key d_{ij});

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 7, lines 36-38; singing a message m using di to form the signature $s_i = m^{di} \bmod N_i$); and

transmitting the encrypted data message (see column 7, lines 39-40; figure 2, step 212; transmitting the signed message s_i).

As per claim 17, Ganesan et al. depicts a communication system for securely transmitting a data message, comprising:

a memory (see column 5, lines 45-46; storing a key portion in a memory);

a processor configured to execute the steps (see column 4, line 66; a user station which includes a processor) comprising:

obtaining a first encrypting key (see column 7, lines 5-9; figure 2, step 200; generating a private exponent key d_{ij});

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits);

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 7, lines 36-38; singing a message m using di to form the signature $s_i = m^{di} \bmod N_i$); and

a transmitter (see column 4, lines 66-67; column 5, lines 1-3; a user station including a transmitter) for transmitting the encrypted data message (see column 7, lines 39-40; figure 2, step 212; transmitting the signed message s_i).

As per claims 18 and 19, Ganesan et al. further show:

that the encryption step corresponds to an RSA public key encryption scheme (see column 7, lines 35-39; figure 2, step 210; signing the message with a private RSA key).

As per claim 24, Ganesan et al. then explain:

a receiver configured to receive the encrypted data message (see column 5, lines 4-5; a server with the capability of receiving transformed messages); and

a second processor (see column 7, lines 1-2; a server with a processor to perform verification) configured to execute:

obtaining a first decrypting key (see column 7, lines 5-9; figure 2, step 200; generating the public and private exponent key d_{ij});

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key to obtain d_j so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 40-47; figure 2, steps 214 and 216; performing signature verification including jointly signing the signed message $s_{ij} = s_i^{dji} \bmod N_i$ with dj and completing the verification by decrypting s_{ij} to verify that $s_{ij}^{eij} \bmod N = m^{didjeij} \bmod N_{ij} = m$).

As per claim 25, Ganesan et al. depict a communication system for securely receiving a data message, comprising:

a memory (see column 6, lines 65-66; servers with memory containing databases; see column 4, lines 63-65; storing the second portion of the private key);

a receiver configured to receive the encrypted data message (see column 5, lines 4-5; a server with the capability of receiving transformed messages);

a receiver configured to receive an encrypted data message (see column 5, lines 1-3; a system server with a receiver to receive transmitted transformed messages);

a processor (see column 7, lines 1-2; a server with a processor to perform verification) configured to execute:

obtaining a first decrypting key (see column 7, lines 5-9; figure 2, step 200; generating the public and private exponent key d_{ij});

generating a second decrypting key as a function of the first decrypting key and as a function of the identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key to obtain d_j so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits); and

decrypting the encrypted data message using the second decrypting key to recover the data message (see column 7, lines 40-47; figure 2, steps 214 and 216; performing signature verification including jointly signing the signed message $s_{ij} = s_i^{dji} \bmod N_i$ with dj and completing the verification by decrypting s_{ij} to verify that $s_{ij}^{eij} \bmod N = m^{didjcij} \bmod N_{ij} = m$).

As per claims 26 and 27, Ganesan et al. further explain:

that the decrypting step corresponds to an RSA public key scheme (see column 7, lines 35-39; figure 2, step 210; signing the message with a private RSA key).

As per claim 32, Ganesan et al. also elaborate:

a transmitter (see column 4, lines 66-67; column 5, lines 1-3; a user station including a transmitter) configured to transmit the encrypted data message (see column 7, lines 39-40; figure 2, step 212; transmitting the signed message s_i);

a second processor configured to execute the steps (see column 4, line 66; a user station which includes a processor) comprising:

obtaining a first encrypting key (see column 7, lines 5-9; figure 2, step 200; generating a private exponent key d_{ij});

generating a second encrypting key as a function of the first encrypting key and as a function of an identified parameter (see column 7, lines 19-22; figure 2, step 202; dividing the private key so that the key portion d_i has a bit length no longer than fifteen percent of the bit length of modulus N, but not less than 56 bits); and

encrypting the data message using the second encrypting key to generate an encrypted data message (see column 7, lines 36-38; singing a message m using di to form the signature $s_i = m^{di} \bmod N_i$).

Claim Rejections - 35 USC § 103

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. Claims 6, 22, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al., U.S. Patent No. 5,341,425 A as applied to claims 1, 17, and 33, respectively, above, and further in view of Ng et al., U.S. Patent No. 5,581,614 A.

Wasilewski et al. teach the methods of claims 1 and 33 and the communication system of claim 17. However, they do not explicitly disclose that the identified parameter is a time or a time-dependent value.

Ng et al. describe:

generating an encrypting key as a function of a time or a time-dependent value(see column 9, lines 13-19; figure 8A, step 314; a key is generated in part on the date of the month previous to the month of transmission).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine any of the methods and system of Wasilewski et al. with the time or time-dependent value of Ng et al. to control access to the information to only authorized users (see column 1, lines 58-61).

27. Claims 14 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al., U.S. Patent No. 5,341,425 A as applied to claims 9 and 25, respectively, above, and further in view of Ng et al., U.S. Patent No. 5,581,614 A.

Wasilewski et al. teach the method of claim 9 and the communication system of claim 25. However, they do not explicitly disclose that the identified parameter is a time or a time-dependent value.

Ng et al. describe:

generating a decrypting key as a function of a time or a time-dependent value (see column 10, lines 30-37; figure 9A, step 374; a key is generated in part on the date of the month previous to the month of transmission).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method or system of Wasilewski et al. with the time

or time-dependent value of Ng et al. to control access to the information to only authorized users (see column 1, lines 58-61).

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 until mid October 2004, then (571) 272-3801 thereafter, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830 until mid October 2004, then (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the

application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900 until mid October 2004, then (571) 272-2100 thereafter.

September 30, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100